Poznań, Poland, 19.01.2022 r.

Rimedo Labs joins 5gSTAR, a 5G cybersecurity project

Rimedo Labs joins forces with the Military institute of Communications (Wojskowy Instytut Łączności), Politechnika Poznańska and Grandmetric to work on 5gSTAR, an innovative research project funded by Narodowe Centrum Badań i Rozwoju on cyber-secuirty in 5G radio access networks.

Rimedo Labs has joined the team implementing the 5gSTAR project on "*Advanced methods and techniques for identification and counteracting cyber-attacks on 5G access network and applications*". The project is funded within the 4th CyberSecIdent program - Cybersecurity and e-Identity by the National Centre for Research and Development in 2021-2024. The goal of the program is to increase the level of cybersecurity by designing the hardware and software aimed at detecting and preventing cyberattacks.

The main goal of the project is to develop methods and techniques for identifying and counteracting new, advanced attacks on access infrastructure and 5G applications. The implementation of the 5gSTAR system will directly contribute to increasing the level of cyberspace security in the Republic of Poland. In particular, the project will focus on 5G application scenarios requiring very low latency and/or very high reliability (URLLC), i.e., those that fit into modern Industry 4.0 installations. As part of the project, elements of detection (probe, honeypot) and counteracting attacks (application firewall, firewall, security policy) will be developed, as well as a security monitoring application allowing for risk assessment and reporting. The developed system will enable integration with client systems, offering protection of ICT infrastructure, detection of threats, protection of privacy, confidentiality, integrity, and availability. Consequently, it will allow the implementation of safe ICT products and services in cyberspace, especially in the area of key service operators. The project will be of an interdisciplinary nature, focusing both on the attacks observed in layers 1-3 and 4-7 of the ISO / OSI model. It is assumed that the methods of analyzing large data sets (collected from sensors placed at various points in the network), statistical analysis algorithms, and artificial intelligence will be used. The sensors planned to be developed (probe, honeypot) will use novel, innovative algorithms that significantly contribute to the development of knowledge in the field of the 5G network security. The monitoring application will use a cognitive approach, presenting the most important information in a transparent manner, allowing the operator to quickly acquire the state of the system and take appropriate action.

As part of the project, Rimedo Labs team will investigate new identification methods and counteracting tactics for cyber-attacks on 5G RAN and Open-RAN. The team will also implement, and test these new algorithms in real-world scenarios. The developed system will enable integration with client systems, offering protection of ICT infrastructure, detection of threats, protection of privacy, confidentiality, integrity, and availability. Consequently, it will allow the implementation of safe ICT products and services in cyberspace, especially in the area of key service operators.

"5G is built almost entirely with software. As a result, it is subject to exploitation, attack, and disruption by hackers and other malicious actors, perhaps including states. 5G will connect much of our lives and business, therefore it will become an attractive target. That is why when it comes to 5G networks, so much

of the focus is on cyber security." said Prof. Hanna Bogucka, Head of Cooperation and Board Member at Rimedo Labs, "We are happy to contribute to the 5gSTAR."

"Military Communications Institute was looking for an experienced subcontractor with the required professional expertise in the field of 5G radio access threat landscape. We are overjoyed we have found Rimedo Labs and look forward to achieving interesting results," says dr Joanna Śliwa, Head of C4I Systems' Department at Military Communications Institute (Wojskowy Instytut Łączności).

"At Grandmetric, we have been working for many years on increasing network access security in the private sector. The perspective of commercial applications of 5G networks will bring new requirements in the area of infrastructure control. We want to help the private sector through the 5G-STAR research project, combining our experiences with the expertise of Wojskowy Instytut Łączności, Rimedo Labs, and Poznan University of Technology," – says Marcin Bialy, Grandmetric's Board Member.

About Rimedo Labs

RIMEDO Labs specializes in providing high-quality and substantive consulting, implementation, and R&D services in the field of modern wireless systems. We implement this through an individual and open approach to the client, constantly improving the team operationally and substantively, updating knowledge and a unique combination of science and business applications. RIMEDO Labs is a spin-off from the Poznan University of Technology, Poland from the Institute of Radiocommunications. In addition to the industrial and implementation projects using a licensed know-how solution in the field of effective allocation of resources in wireless networks, RIMEDO Labs also provides consulting and education in the field of O-RAN. The company's clients and partners are and can be both domestic and foreign entities with various profiles. For more information, please visit https://www.rimedolabs.com/

RIMEDO Labs
ul. Polanka 3, 61-131 Poznań, Poland
Tel.: +48 61 665 38 17
rimedolabs.com
info@rimedolabs.com